UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,056	12/30/2003	Charles Douglas Ball	RPS920030201US1	8331

61755   7590   06/26/2008
Kunzler & McKenzie
8 EAST BROADWAY, SUITE 600
SALT LAKE CITY, UT 84111

EXAMINER
SCHMIDT, KARI L

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
06/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2008*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-11,14-17,19-24 and 26-30* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-11,14-17,19-24 and 26-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 03/10/2008.

Claims 1, 4-11, 14-17, 19-24 and 26-30 remain pending. Claims 2-3, 12-13, 18 and 25

have been canceled. Claims 1, 8, 11, 17, 24 and 30 have been amended.

Response to Arguments

Applicant's arguments filed 10 March 2008 have been fully considered but they

are not persuasive.

The applicant argues that new amendments made to independent claims 1, 8,

11, 17, 24, and 30 overcome the cited references of Ilnicki in view of Brickell. The

examiner disagrees for the following reasons:

The examiner notes with respect to the first amendment "... the enables the

secure function module ...," the examiner notes Ilnicki discloses a secure function

module "that enables the secure function module" (see at least, column 2, lines 42-55,

Figure 1: the examiner notes the browser) to transact functions with an excluding

computing module (see at least, col. 2, lines 42-55, Figure 1: the examiner notes the

measuring agent to be the excluding module) with the use of the public key of the

measuring agent (see at least, column 6, line 47-column 7, line 41). The examiner notes

under the broadest reasonable interpretation one of ordinary skill in the can interpret

this to be enabling the secure function module to transact secure functions with an

excluding computing module.

The examiner notes with respect to the second and third amendments of "... 'that enables the secure function module' to transact secure functions with a non-conforming computing module comprising storing cryptographic keys for the non-conforming computing module 'wherein the non-conforming computing module cannot transact the secure function with the secure function module using the cryptographic keys of the excluding computing module'," the examiner notes Ilnicki discloses enabling the secure function module (see at least, col. 4, lines 6-10: the examiner notes an browser to be the secure function module) to transact with the secure functions with a non-conforming module (see at least, col. 6, line 47-col. 7, line 31 and Figure 4: the examiner notes the "browser launching the agent" this agent being in a non-secure environment (different from the first agent representing the ECM)) with the use of the public key of the given measuring agent (see at least, column 6, line 47-column, 7, line 41). The examiner would like to note that each key is unique to a given agent therefore it would read on the amendment of 'wherein the non-conforming computing module cannot transact the secure function with the secure function module using the cryptographic keys of the excluding computing module' due to each key being unique for each agent (see at least, column 6, line 47-column 7, line 41). The examiner notes under the broadest reasonable interpretation one of ordinary skill in the can interpret this to be the non-confirming computing module only using its own key and not the key of the ECM.

The examiner notes with respect to the fourth amendment and fifth amendments of "... 'so that the non-conforming computing module must transact the secure function through the excluding computing module' ... 'and unable to transact the secure function

module through the excluding module' ..." are contradicting. The examiner has noted

this in the 35 USC 112 rejection, found in the office action. How can the non-

conforming module both "must" transact and then not be able to transact? The

examiner has provided the interpretation from Ilinki that the secure computing module

(see at least, Figure 1 and Figure 4: the examiner notes the browser) to be able to be

configured to communicate both with the excluding conforming module (see at least,

col. 2, lines 42-55 and Figure 1: the examiner notes transferring of data through the

agent to the browser) and the non-confirming computing module (see at least, Figure 4

and column 4, lines 21-29: transferring data between agent through the browser through

the non-trusted node). The examiner notes under the broadest reasonable

interpretation one of ordinary skill in the can interpret this to be enabling the secure

function module to communicate with both modules.

   With respect to the sixth and seventh amendments of "a context module

configured to 'identify the excluding module and initiating the secure function ... and to

identify the non-conforming computing module initiating the secure function ...," the

examiner notes Ilnicki discloses that the that in the case of a trusted environment

secure connection is handled by the agent to the browser and in the a non trusted

environment the agent communicates via the browse based on the non-trusted

environment (see at least, col. 10, lines 55-64). So in either environment trusted or non-

trusted the modules will initiate secure functionality based on the environment they are

in. The examiner notes under the broadest reasonable interpretation one of ordinary

skill in the can interpret this to be each module configured to initiate a secure function

with respect to their environment.

The examiner has noted that Ilnicki does indeed teach the new amendments

made to the independent claims, therefore the arguments of not teaching the new

claimed limitations, are not persuasive.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claims 1, 4-11, 14-17, 19-24, and 26-30 rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention.

The examiner notes the limitation found in the independent claims of "... 'so that

the non-conforming computing module must transact the secure function through the

excluding computing module' ... 'and unable to transact the secure function module

through the excluding module' ..." are contradicting. The examiner is confused on how

the secure function module communicate must communicate through the non-

conforming via the excluding computing module and then unable to transact the secure

function through the excluding computing module? The examiner will interpret the

secure function module to be able to be configured to communicate both with the

excluding conforming module.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-11, 14-17, 19-24, and 26-30 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Ilnicki et al. (7,069,434 B1) in view of Brickell (US

2005/0069135 A1).

Claim 1, 8, 11, 17, 24 and 30

Ilnicki discloses a secure data processing device comprising: a secure function module

configured to receive an excluding computing module context (see at least, column 2,

lines 42-55, Figure 1, browser and measuring agent), that enables the secure function

module to transact secure function with an excluding computing module comprising

storing cryptographic keys for the excluding computer(see at least, Figure 1, column 2,

lines 42-55 and col. 6, lines 47-col. 7, lines 1-41: the examiner notes that the measuring

agent resides in the browser which would receive secure content to transact);

the secure function module further configured to receive a non-conforming computing

module context (see at least, Figure 4, column 4, lines 6-10: Agent), that enables the

secure function to transact secure functions with a non-conforming computing module

comprising storing cryptographic keys for the non-conforming computing module

wherein the non-conforming computing module cannot transact the secure function with

the secure function module using cryptographic keys of the excluding computing

module (see at least, and col. 6, lines 47-col. 7, lines 1-41 and Figure 4: "the browser

launches agent"); a communication module configured to communicate with the

excluding computing module, the excluding computing module configured to

exclusively transact the secure function with the secure function module so that the non-

conforming computing module must transact the secure function through the excluding

computing module (see at least, column 2, lines 42-55 and col. 6, lines 47-col. 7, lines

1-41), the communication module further configured to communicate with the non-

conforming computing module, the non-conforming computing module configured to

transact the secure function with the secure function module and usable to transact the

secure function through the excluding computing module(see at least, Figure 4, column

4, lines 21-29: "transferring data between an application server and an agent of the

application server through a non-trusted node"); and a context module configured to

identify the excluding computing module initiating the secure function and set the

context of the secure function module to the excluding computing module context and to

identify the non-conforming computing module initiating the secure function and set the

context of the secure function module to the non-conforming computing module context

(see at least, column 10, lines 55-64: the examiner notes in a case of a non trusted

environment the agent communicates via the non conforming computing module, in a

case of a trusted environment communicates via the secure connection all handled by

the Agent).

Ilnicki fails to disclose the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules.

However Brickell discloses the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules (see at least, [0031], [0032],[0042], [0079]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ilnicki to include the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules as taught by Brickell. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a reliable and secure exchange of information in modern communication systems (see at least, [0002]).

Claim 4

Ilnicki discloses the device of claim 1, wherein context module is configured to arbitrate the setting of the context of the secure function module to either the excluding computing module context or to the non-conforming computing module context (see at least, column 10, lines 55-64: the examiner notes in a case of a non trusted environment the agent communicates via the non conforming computing module, in a case of a trusted environment communicates via the secure connection all handled by the Agent).

Claim 5

Ilnicki discloses the device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to an electrical signal (see at least, Figure 4: the examiner notes the browser launching the agent is interrupt to be an electrical signal residing in a computer).

Claim 6

Ilnicki discloses the device of claim 5, wherein the electrical signal is an address (see at least, Figure 4: the examiner notes the agent communicating to the web server via the launch of the browser to be an electric signal containing an address).

Claim 7

Ilnicki discloses the device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to data communicated to the communication module (see at least, column 10, lines 55-64: the examiner notes in a case of a non trusted environment the agent communicates via the non conforming computing module, in a case of a trusted environment communicates via the secure connection all handled by the Agent).

Claim 9

Ilnicki discloses the module of claim 8, the identification module further configured to identify the excluding computing module and non-conforming computing module with an

address communicated from the address module (see at least, Figure 4: the examiner

notes agent derives shared secret from its and apps public keys and the browser

launches agent).

Claim 10

Ilnicki discloses the module of claim 8, the identification module further configured to

identify the excluding computing module and non-conforming computing module with

data communicated from the data module (see at least, Figure 4: the examiner notes

agent derives shared secret from its and apps public keys and the browser launches

agent).

Claim 14, 21 & 27

Ilnicki discloses the system of claim 11, wherein the secure function module identifies

the excluding computing module and non-conforming computing module from an

electrical signal (see at least, Figure 4: the examiner notes the browser launching the

agent is interrupt to be an electrical signal residing in a computer).

　　　Ilnicki fails to disclose the device configured as a Trusted Platform Module (TPM)

which is configured to use and store cryptographic keys to transact secure functions

with modules.

　　　However Brickell discloses the device configured as a Trusted Platform Module

(TPM) which is configured to use and store cryptographic keys to transact secure

functions with modules (see at least, [0031], [0032],[0042], [0079]).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the teachings of Ilnicki to include the device configured as

a Trusted Platform Module (TPM) which is configured to use and store cryptographic

keys to transact secure functions with modules as taught by Brickell. One of ordinary

skill in the art would have been motivated to combine the teachings in order to provide a

reliable and secure exchange of information in modern communication systems (see at

least, [0002]).

Claim 15, 22 & 28

Ilnicki discloses the system of claim 14, wherein the electrical signal is an address (see

at least, Figure 4: the examiner notes the agent communicating to the web server via

the launch of the browser to be an electric signal containing an address)..

Claim 16, 23 & 29

Ilnicki discloses the system of claim 11, wherein the secure computing module identifies

the excluding computing module and non-conforming computing module from a data

value (see at least, Figure 7: "collective measured data").

Ilnicki fails to disclose the device configured as a Trusted Platform Module (TPM)

which is configured to use and store cryptographic keys to transact secure functions

with modules.

However Brickell discloses the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules (see at least, [0031], [0032], [0042], [0079]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ilnicki to include the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules as taught by Brickell. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a reliable and secure exchange of information in modern communication systems (see at least, [0002]).

Claim 19, 20 & 26

Ilnicki discloses the system of claim 17, wherein the excluding computing module and the non-conforming computing module transact the secure function with secure computing module (see at least, column 10, lines 55-64: the examiner notes in a case of a non trusted environment the agent communicates via the non conforming computing module, in a case of a trusted environment communicates via the secure connection all handled by the Agent).

Ilnicki fails to disclose the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules.

However Brickell discloses the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules (see at least, [0031], [0032], [0042], [0079]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ilnicki to include the device configured as a Trusted Platform Module (TPM) which is configured to use and store cryptographic keys to transact secure functions with modules as taught by Brickell. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a reliable and secure exchange of information in modern communication systems (see at least, [0002]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

/Kari L Schmidt/
Examiner, Art Unit 2139